

## Tabla de Contenidos

CERTuy.....	1
Guía Rápida de Instalación y Uso de GnuPGP.....	1
1 Objetivo .....	3
2 Descripción de la Herramientas.....	3
3 Instalación de las herramientas.....	4
3.1 GPG4Win.....	4
3.2 Thunderbird + Enigmail:.....	5
3.3 Outlook: .....	5
4 Uso de las Herramientas.....	6
4.1 Generar una clave.....	6
4.2 Compartir la clave.....	7
4.2.1 Exportar la Clave.....	8
4.2.2 Enviarla a un Servidor.....	8
4.3 Firmar y encriptar Correos y Archivos.....	10
4.3.1 Correos con Thunderbird.....	10
4.3.2 Correos con Outlook.....	12
4.3.3 Archivos.....	14
5. Referencias .....	15

## 1 Objetivo

Ser una guía rápida para la instalación y utilización de las herramientas de firma y encriptado de mails y archivos de licenciamiento open source “GNU Privacy Guard” -GnuPG ó GPG- y los correspondientes add-ins para las herramientas de correo Mozilla Thunderbird 2.0 y Outlook (2003/2007) bajo sistemas operativos Windows XP y Windows Vista.

## 2 Descripción de la Herramientas

GnuPG es una implementación open source del estandard OpenPGP como esta definido por el [RFC4880](#).

La versión de GPG utilizada al momento de elaboración de este documento es la 1.4.9.

Permite encriptar y firmar los datos, realizando un manejo de las claves sencillo y efectivo, así como los módulos necesarios para acceder a los directorios de clave publica existentes en el mundo.

GPG es una herramienta de línea de comando, pero la idea es facilitar su uso desde herramientas de usuario -frontends- las cuáles permiten realizar todas las tareas a través de una GUI.

Para poder encriptar y firmar, GPG genera claves asimétricas para cada usuario, quien es el responsable de generarlas. Para que el proceso funcione correctamente los usuarios deben de intercambiar la clave pública, para ello lo pueden hacer enviándola al otro usuario (mail, archivo, etc) y/o publicarla en los servidores de claves publicas que existen (las herramientas también ayudan en ese sentido).

GPG utiliza algoritmos de software que no se encuentra protegidos por patentes, algunos de ellos son: ELGamal, CAST5, 3DES, AES y Blowfish.

GPG es una herramienta de línea de comando, para frontends (GUI) se pueden utilizar algunos como:

- GPG4Win1.1.4 ó
- GPGShell

Ambas herramientas son de distribución gratuita, si bien se pueden tener las dos herramientas instaladas, se recomienda utilizar [GPG4Win1.1.4](#), esta recomendación es debido a dos facilidades: instala por defecto GnuPG y además los add-ins para Outlook automaticamente.

Para [Thunderbird 2](#) se debe de agregar el add-in de [Enigmail](#).

### 3 Instalación de las herramientas

**NOTA:** Para evitar problemas, la instalación se debe realizar con una cuenta que posea privilegios de Administrador.

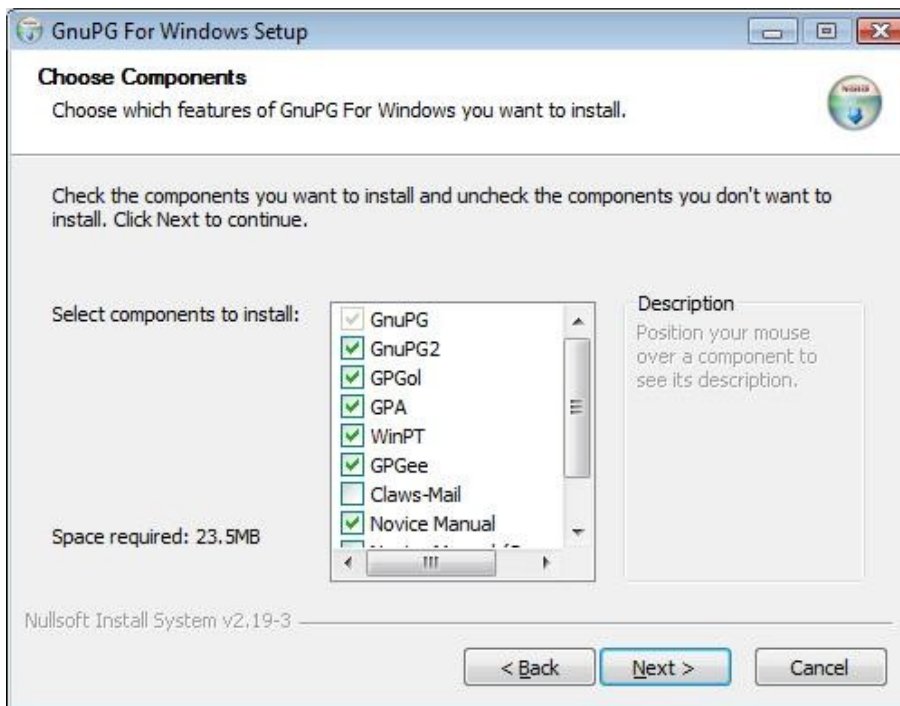
#### 3.1 GPG4Win

<http://www.gpg4win.org/download.html>

Ejecutar gpg4win-1.1.4.exe

Permitir ejecutar (Windows Vista).

Seleccionar que “Sí”, “Siguiente” o “Next” hasta que aparezca la opción: “**Choose Component**” y **dejar solamente marcadas las opciones que acá aparecen (desmarcar el resto: Claws-Mail y manuales en Alemán, hay algunas que no se ven en la imagen porque están más abajo)**.



Continuar con “Next” hasta el final.

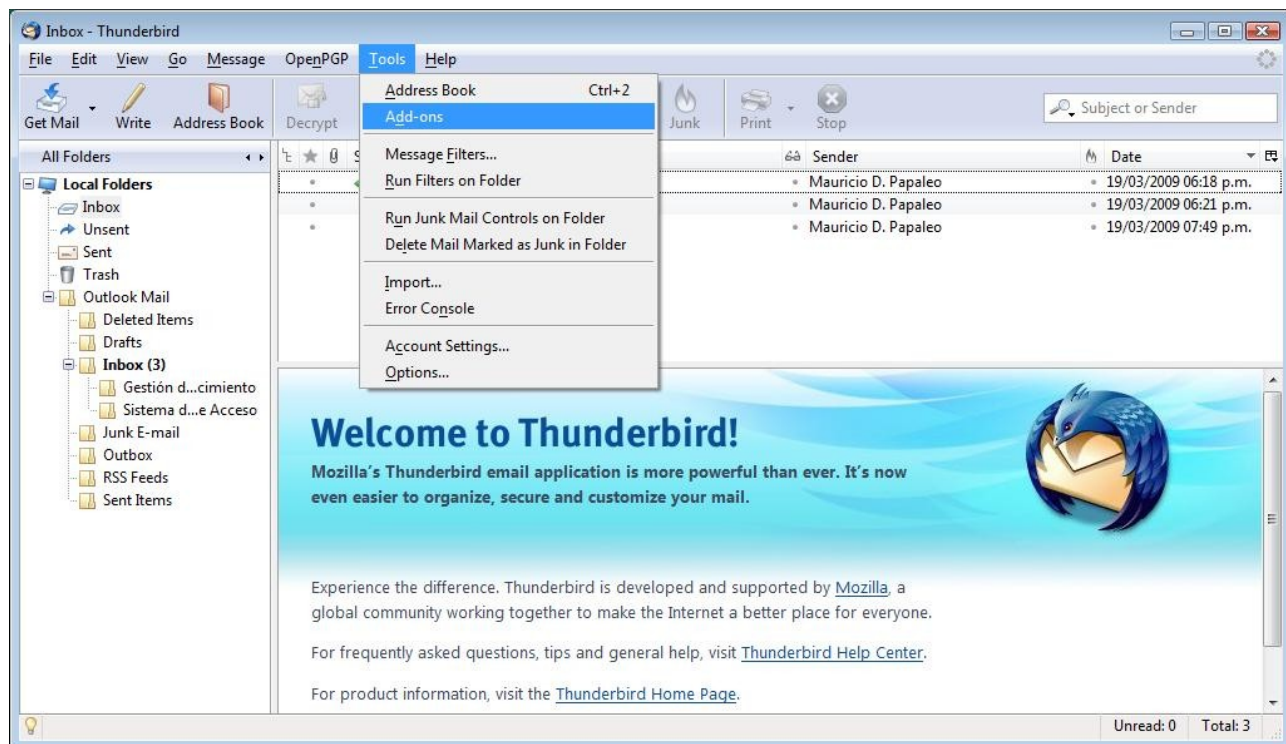
### 3.2 Thunderbird + Enigmail:

Instalar **Thunderbird**.

<http://www.mozillamessaging.com/en-US/thunderbird/>

Luego instalar el add-on de **Enigmail**: enigmail-0.95.7-tb+sm.xpi.

<http://enigmail.mozdev.org/download/index.php>



Luego de dar clic sobre Add-ons, dar clic sobre “Install”, localizar donde se encuentra el archivo .xpi y marcarlo, y dar clic sobre Aceptar y queda listo.

### 3.3 Outlook:

En el caso de Outlook, no se deben de realizar más tareas y se encuentra listo para su utilización.

## 4 Uso de las Herramientas

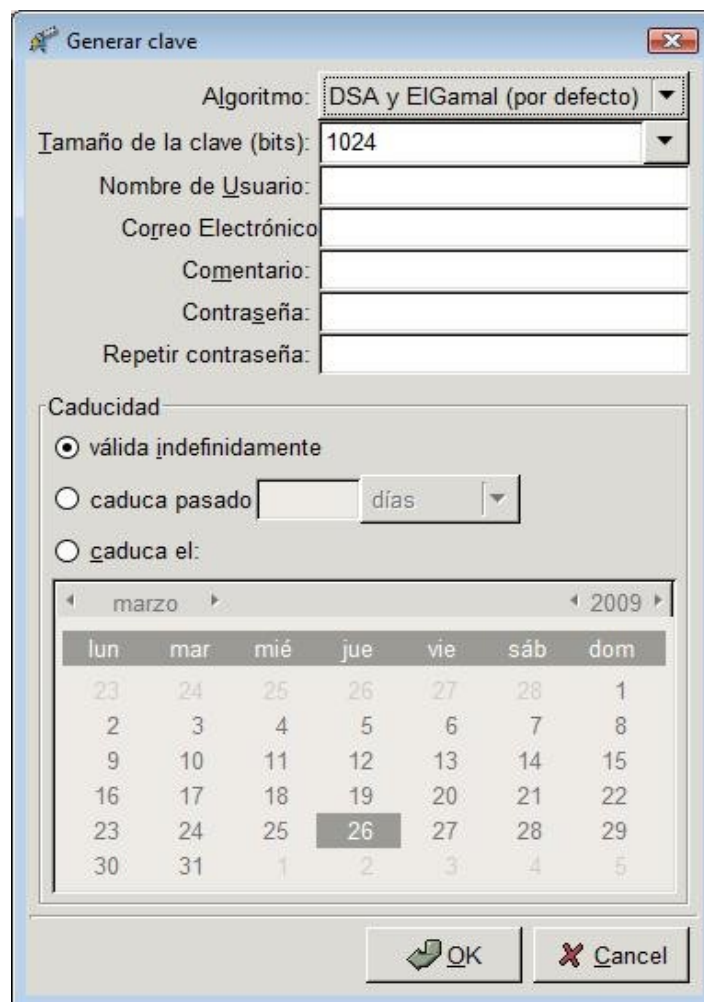
Se explicitarán las acciones más comunes que se realizan con GPG, tales como: generar una clave, compartir la clave, firmar y encriptar un archivo y firmar y encriptar un correo.

### 4.1 Generar una clave

**NOTA: Esta operación solo se debe de hacer una vez por cada clave que se desee crear. Es responsabilidad del usuario proteger de forma adecuada la clave privada.**

Para generar una clave en GnuPG for Windows se debe de ejecutar el programa GPA (Menú Inicio -> Programas -> GnuPG for Windows -> GPA)

Allí se deberá generar la nueva clave:



Generar clave

Algoritmo: DSA y ElGamal (por defecto)

Tamaño de la clave (bits): 1024

Nombre de Usuario:

Correo Electrónico:

Comentario:

Contraseña:

Repetir contraseña:

Caducidad

válida indefinidamente

caduca pasado  días

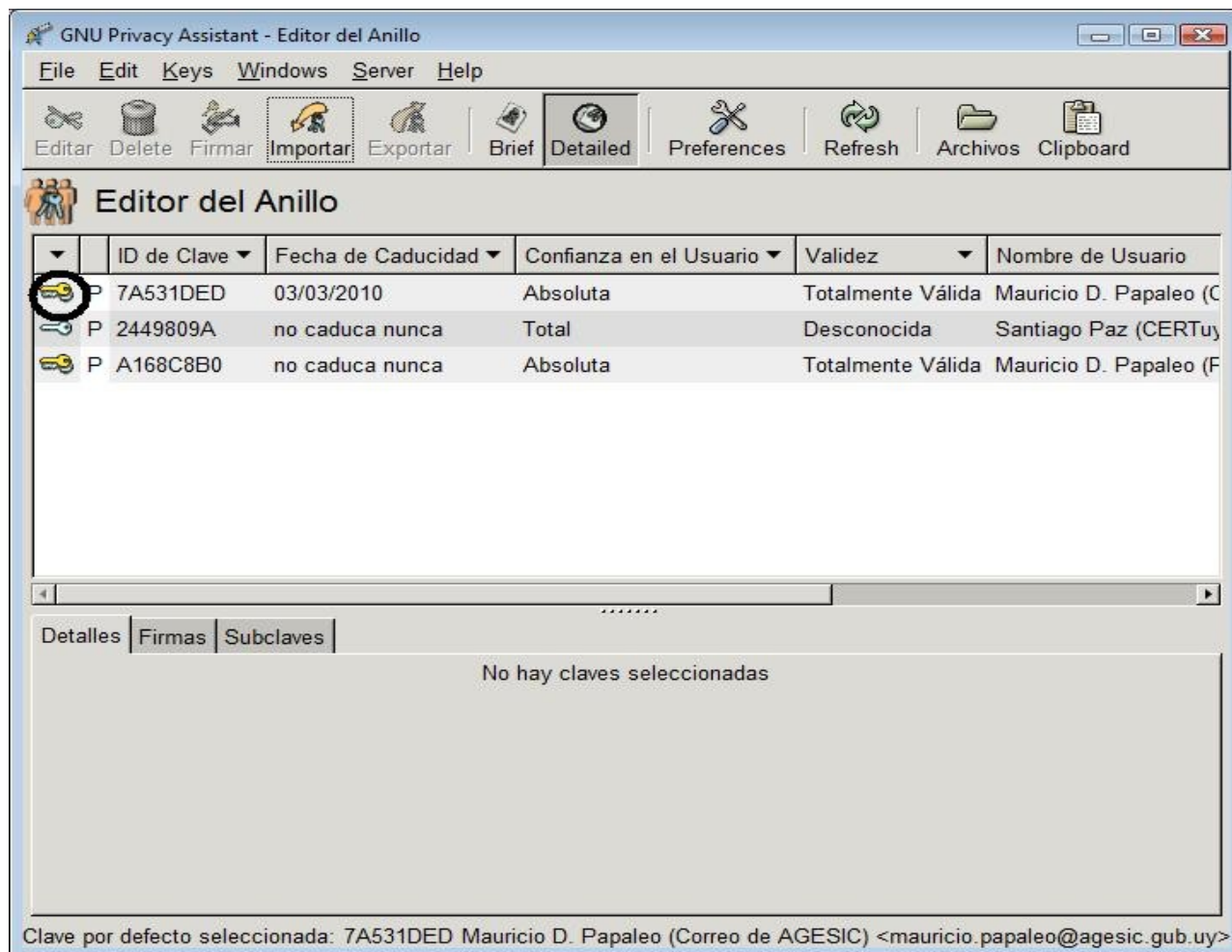
caduca el:

marzo							2009
lun	mar	mié	jue	vie	sáb	dom	
23	24	25	26	27	28	1	
2	3	4	5	6	7	8	
9	10	11	12	13	14	15	
16	17	18	19	20	21	22	
23	24	25	26	27	28	29	
30	31	1	2	3	4	5	

OK Cancel

Seleccione la clave y subclave que considere adecuadas.

Al finalizar, deberá aparecer una pantalla similar a esta (con las dos llaves que aparecen marcadas con una eclipse), las dos llaves indican que se tiene la clave pública y la privada.



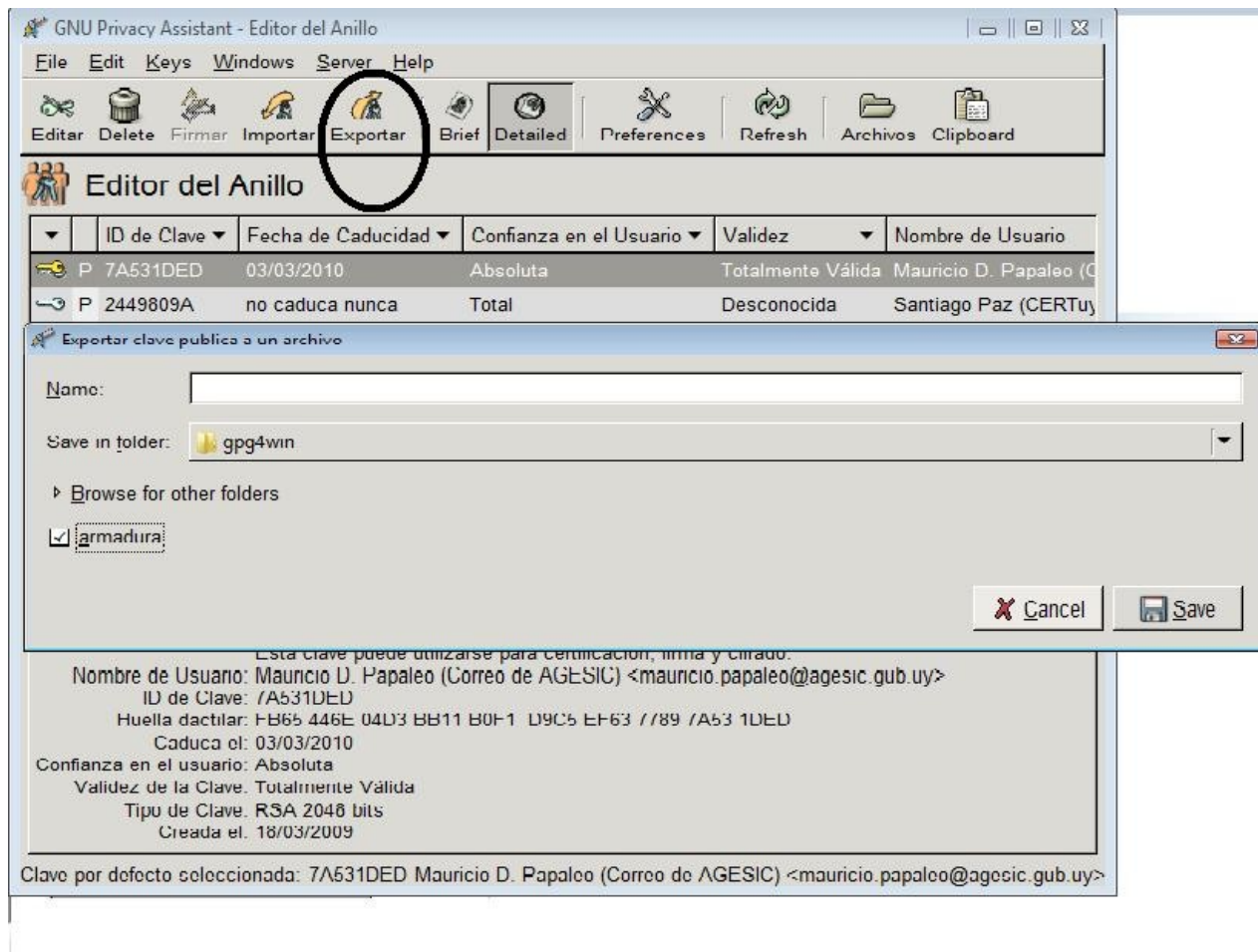
Al llegar a este paso uno ya posee las claves necesarias.

## 4.2 Compartir la clave

Para compartir la clave se debe de exportar la clave pública, dicho procedimiento se puede realizar de dos formas diferentes: o bien exportando la clave publica de forma manual, copiarla en un archivo y/o mail y luego enviarla a las personas que uno considere necesario ó utilizando las herramientas,

enviarlas a un servidor público de claves públicas.

#### 4.2.1 Exportar la Clave

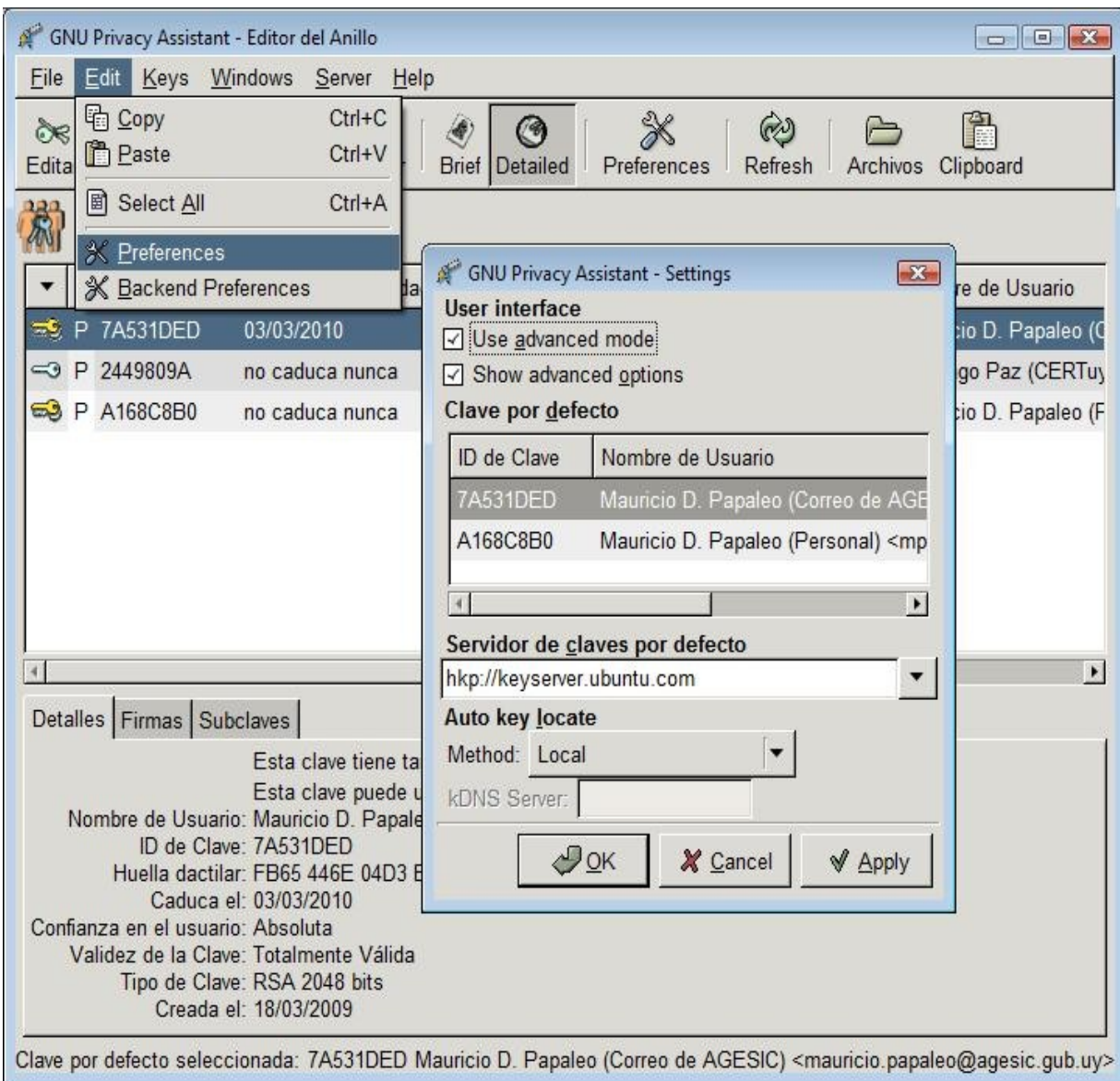


Luego de dar clic sobre Exportar, aparece este box indicando a donde será el camino para dejar la clave pública, se deberá indicar además el nombre y la extensión del archivo, por ejemplo “NombreUsuario.txt”.

Luego se la deberá enviar por correo o por otro medio.

#### 4.2.2 Enviarla a un Servidor

Primero deberá seleccionar el servidor de acuerdo a lo que muestra la figura:



Seleccionar el servidor de claves que desea utilizar por defecto.

Luego de haber realizado esto, se debe de enviar la clave de acuerdo a la siguiente figura:

The screenshot shows the GNU Privacy Assistant - Editor del Anillo interface. A warning dialog box is displayed in the foreground, asking for confirmation to send a selected key to a public keyserver. The dialog text reads: "La clave seleccionada se enviará a un servidor de claves público ('hkp://keyserver.ubuntu.com'). ¿Está seguro de que quiere distribuir esta clave?". There are "Sí" and "No" buttons at the bottom of the dialog.

The background window shows a table of keys with the following columns: ID de Clave, Fecha de Caducidad, Confianza en el Usuario, Validez, and Nombre de Usuario. The selected key is:

ID de Clave	Fecha de Caducidad	Confianza en el Usuario	Validez	Nombre de Usuario
P 7A531DED	03/03/2010			Mauricio D. Papaleo (C...
P 2449809A	no caduca n...			Diago Paz (CERTuy...
P A168C8B0	no caduca n...			Mauricio D. Papaleo (F...

Below the table, the "Detalles" tab is active, showing the following information for the selected key:

- Esta clave tiene tanto una parte secreta como una pública
- Esta clave puede utilizarse para certificación, firma y cifrado.
- Nombre de Usuario: Mauricio D. Papaleo (Correo de AGESIC) <mauricio.papaleo@agesic.gub.uy>
- ID de Clave: 7A531DED
- Huella dactilar: FB65 446E 04D3 BB11 B0F1 D9C5 EF63 7789 7A53 1DED
- Caduca el: 03/03/2010
- Confianza en el usuario: Absoluta
- Validez de la Clave: Totalmente Válida
- Tipo de Clave: RSA 2048 bits
- Creada el: 18/03/2009

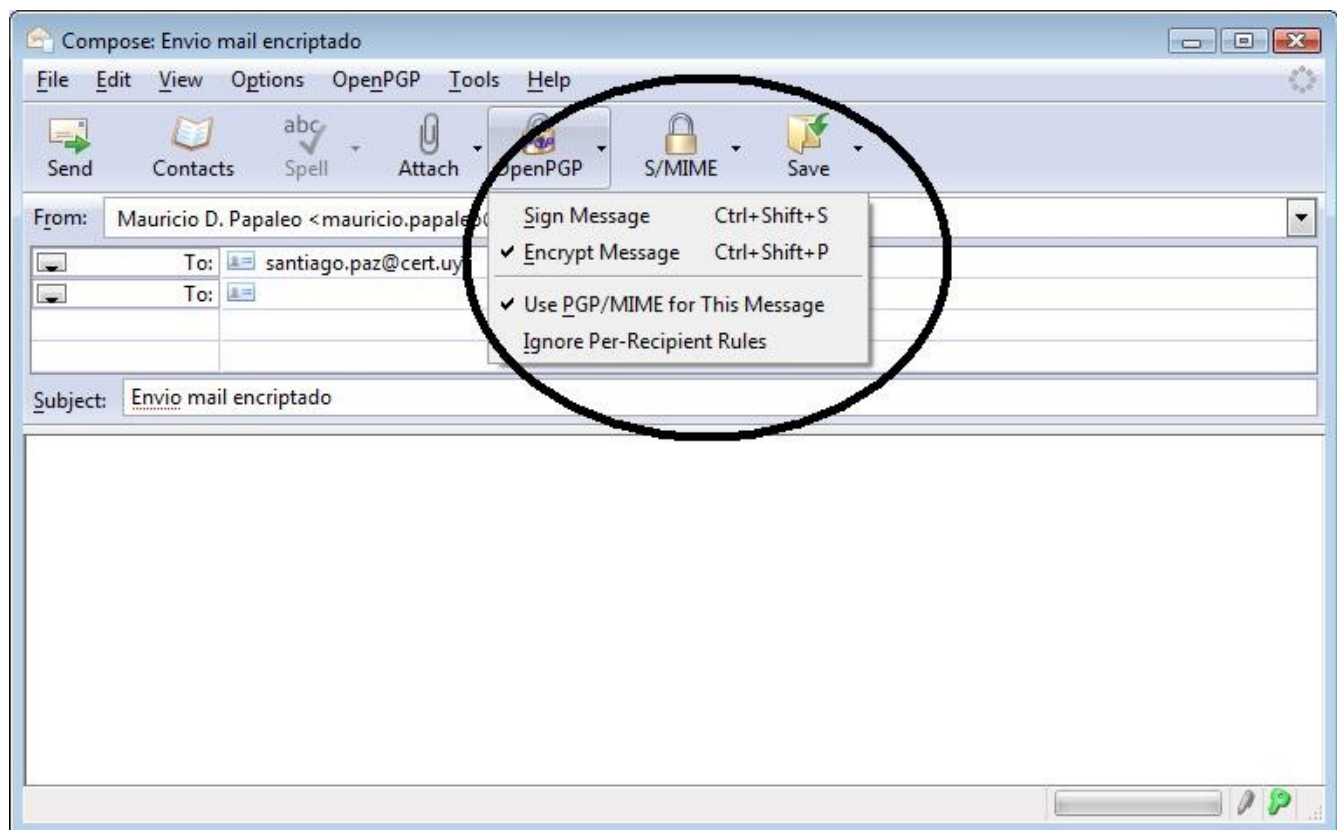
Clave por defecto seleccionada: 7A531DED Mauricio D. Papaleo (Correo de AGESIC) <mauricio.papaleo@agesic.gub.uy>

Al seleccionar "SI", la clave se enviará y quedará publicada en ese servidor.

## 4.3 Firmar y encriptar Correos y Archivos

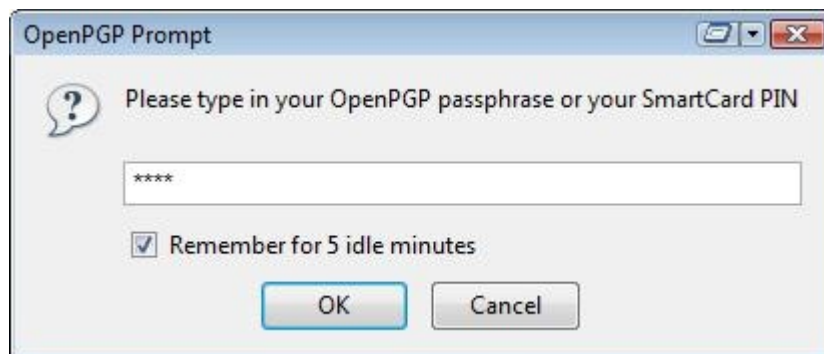
### 4.3.1 Correos con Thunderbird

Para firmar un mail en Thunderbird, se debe abrir Thunderbird, seleccionar Escribir (Write) y se tiene la opción de encriptar, la opción de Firmar y que el formato sea PGP/Mime o no, tal como se ve en la siguiente figura:



A continuación se da Enviar (Send) y funciona como un correo normal, quien lo recibe luego lo tendrá que desencriptar como veremos a continuación.

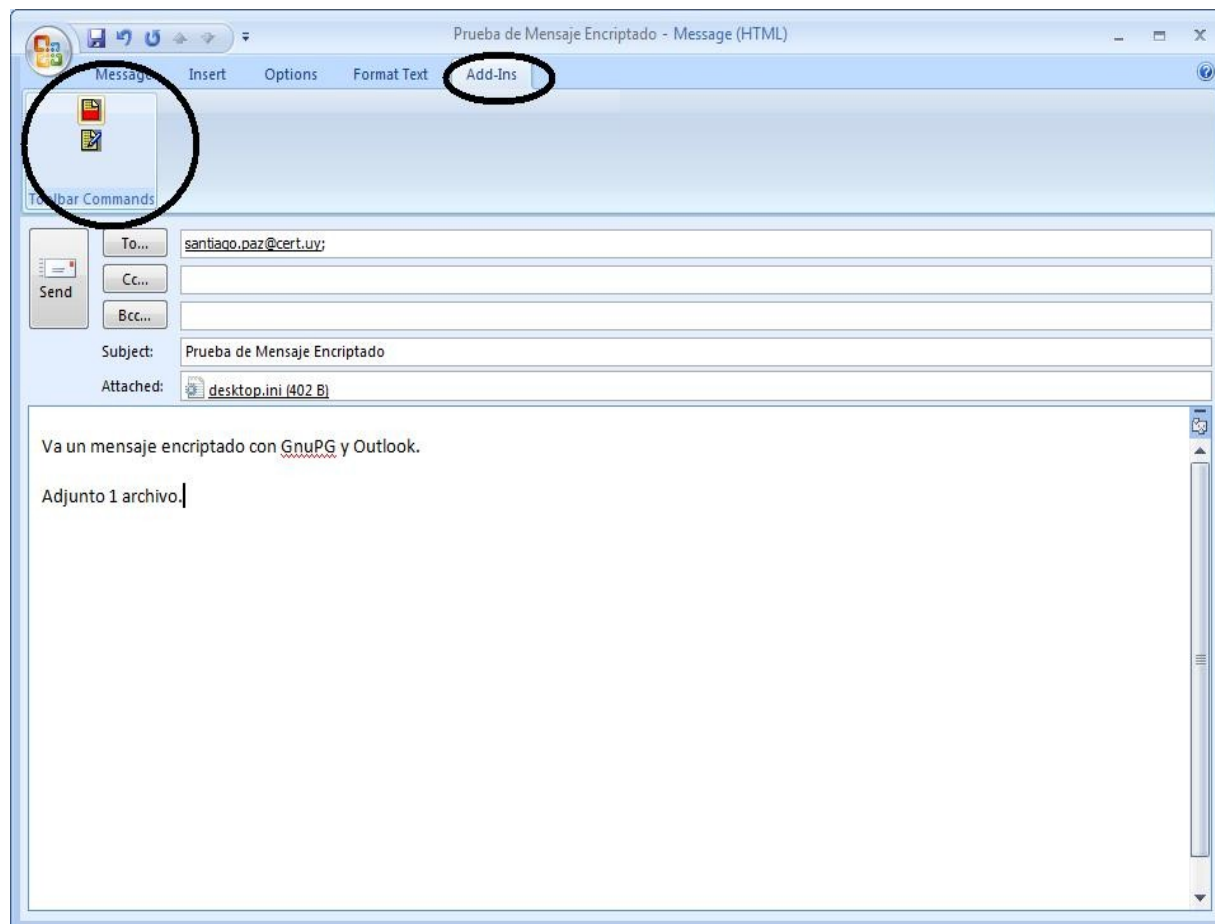
Cuando uno recibe un mensaje encriptado al abrirlo Thunderbird solicitará la contraseña de la clave para poder desencriptar el mensaje, como lo ilustra la figura:



A continuación el mensaje se mostrará como cualquier otro mensaje normal al ser descifrado.

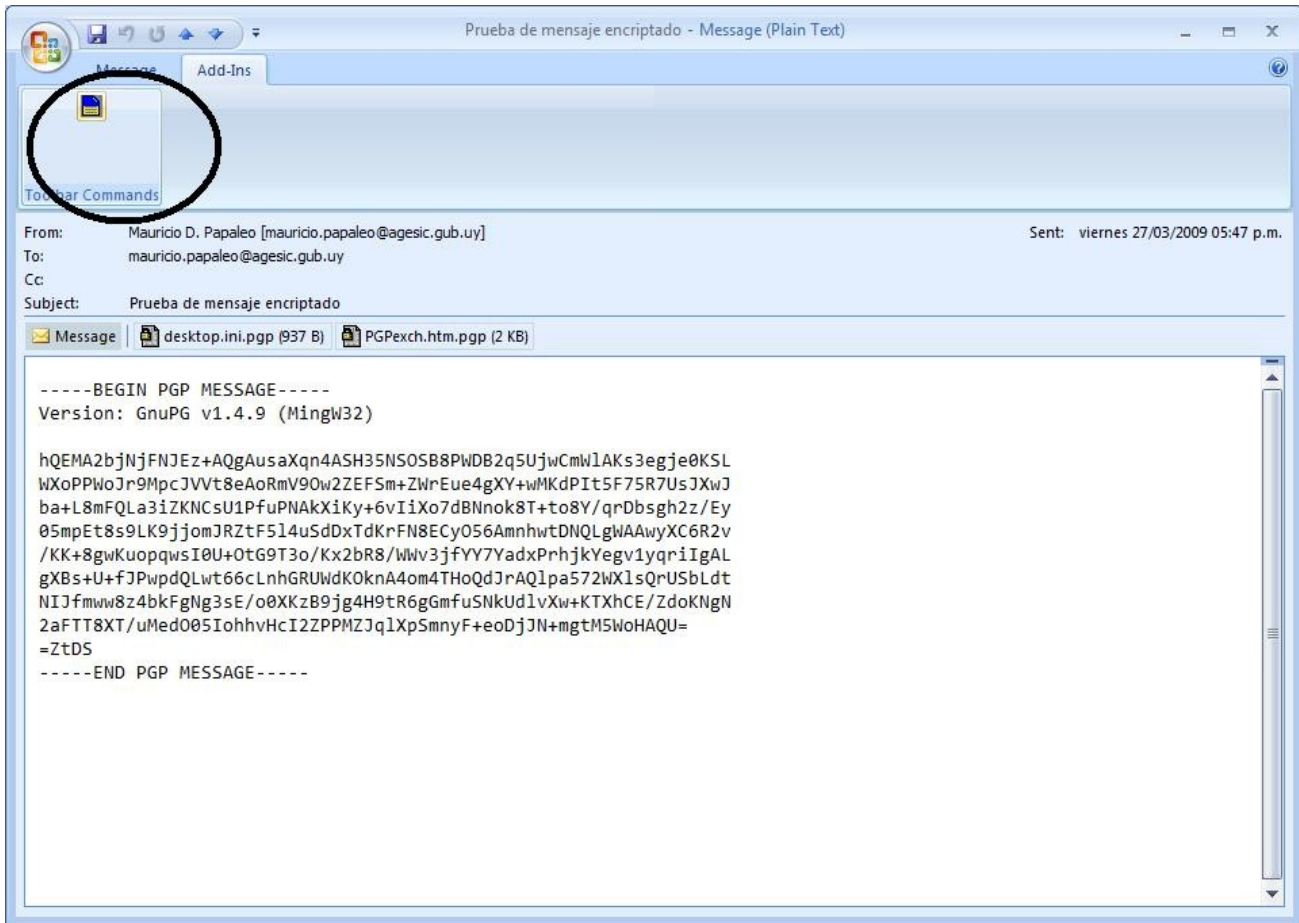
#### 4.3.2 Correos con Outlook

Para firmar un mail en Outlook, luego de abrir el Outlook, vamos a Nuevo (New) y luego de seleccionar destinatario y demás opciones, se debe ir a la barra de menú y ubicar en el menú los Add-ins y seleccionar la operación que se desea realizar: firmar y/o encriptar, tal como se ve en la siguiente figura:

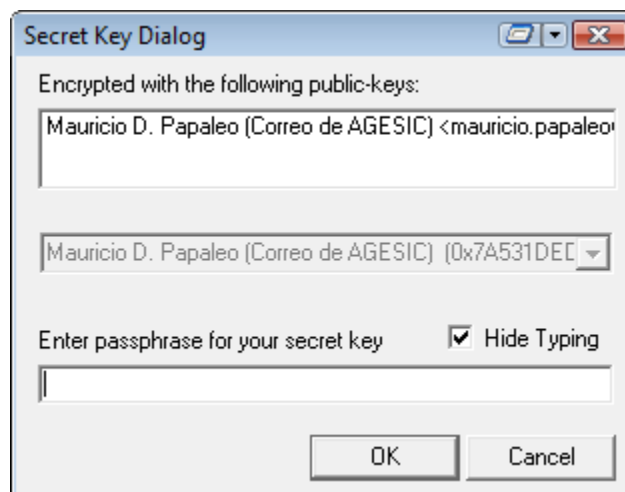


A continuación se da Enviar (Send) y funciona como un correo normal. Quien lo recibe luego lo tendrá que desencriptar correctamente como veremos a continuación.

Cuando se recibe un mensaje encriptado, Outlook por defecto no lo desencripta, para ello, se deberá acceder al Menú de Add-in para seleccionar la opción de desencriptarlo, como lo ilustra la figura:

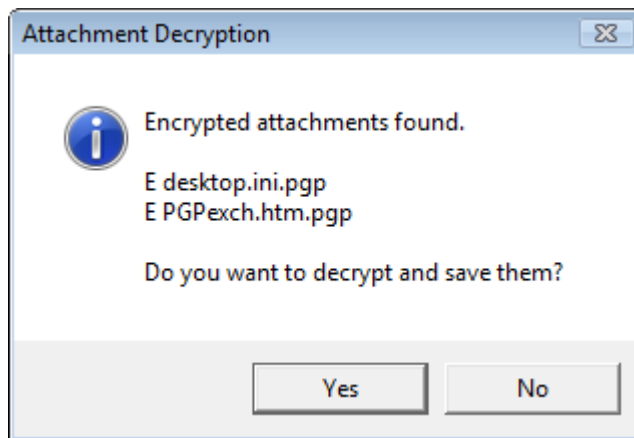


Luego de dar clic sobre el botón de Desencriptar, se presentará la siguiente pantalla:



Al ingresar la contraseña de la clave, si el mensaje no tiene archivos adjuntos, lo muestra descriptado.

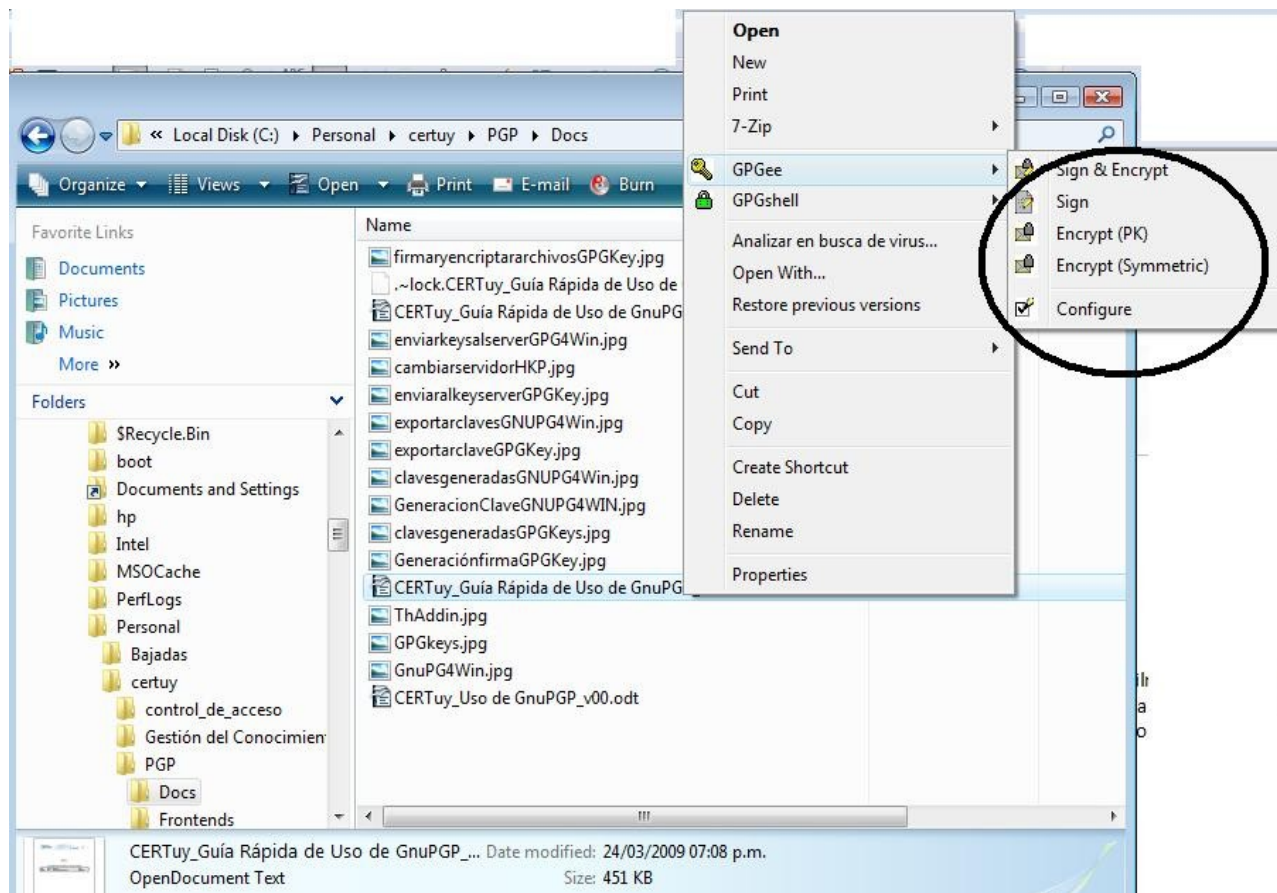
En caso de tener un archivo dentro del mensaje presentara el siguiente cuadro de dialogo:



Al decirle que “Si” (Yes), solicita el camino donde depositar el archivo descriptado. Luego se podrá leer normalmente.

### 4.3.3 Archivos

GnuPG for Windows se integra con el shell de Windows (XP y Vista) y se puede invocar fácilmente en cualquier momento, por ejemplo, al seleccionar un archivo desde el Explorer y cuando se marca un archivo, al dar botón derecho, aparece un menú de contexto donde se puede seleccionar la opción de firmar/criptar ó firmar y encriptar, de acuerdo como lo muestra la figura:



## 5 Referencias

CSIRT ANTEL – CA004-gstillo-Us0-GPG.pdf

GPG4Win - Gpg4win for Novices.pdf v1.0.0 Nov 2006

The GNU Privacy Handbook - <http://www.gnupg.org/gph/en/manual.html>